Improve network capacity on Multi-hop 802.11-based wireless networks

A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols.

Improve network capacity (Future Work)

A Thesis
Submitted to the Department of Computer Science and Engineering
of
BRAC University
by

Niti Jabin
Student ID: 03201050
Tasnuva Sumaiya
Student ID: 02201042

In Partial Fulfillment of the requirements for the Degree
of
Bachelor of Science in Computer Science
Fall 2007

DECLARATION

I hereby declare that this thesis is based on the results found by ourselves. Materials of work found by other researcher are mentioned by reference. This thesis, neither in whole nor in part, has been previously submitted for any degree.

Signature of
Supervisor

_____
Sadia Hamid Kazi

Students' names & Signatures:

_____
1. Tasnuva Sumaiya

_____
2. Niti Jabin

ACKNOWLEDGMENTS

First of all we would like to thank our supervisor Ms. Sadia Hamid Kazi for all the freedom and guidance she in every possible way through this exertion. She arranged all the facilities and the necessary supports, which were indispensable for our thesis.

We would also like to thank our co-supervisor Mr. Risat Mahmud Pathan for his cordial co-operation. His profound knowledge, keen interest, patience, and the support have served as the impetus for us to carry out the task.

Finally, we also thank our families and all our friends, especially those, who supported us with their valuable suggestion and encouragements.

ABSTRACT

This thesis report seeks to study and analyze in-depth regarding various medium access control (MAC) layer algorithms and protocols that have been implemented and proposed for wireless networks and shows a performance comparison of three mobile ad-hoc network with an intention to improve wireless network capacity. Theory begins with a short overview of wireless network and its type like infrastructure base network, wireless personal area network (WPAN), wireless sensor network (WSN) and wireless cellular networks, infrastructure less network. Then short overview of basic MAC algorithms used in wireless medium access control layer. Then special MAC algorithms for world of wireless are discussed. A detailed description of mobile ad-hoc network and its protocols. Finally, it shows performance comparison of three routing protocols of MANET. Using network simulator ns-2 it shows the simulation result.

CONTENTS

1 INTRODUCTION

1.1 Wireless Communication.....9

1.2 Wireless Network.....11

Types of Wireless Networks.....12

2 MEDIUM ACCESS CONTROL.....13

2.1 MAC Protocols ……13

2.1.1 Basic MAC Algorithms.....13

i. ALOHA.....14

ii. CSMA 15

2.1.2 BACK-OFF ALGORITHMS 16

i. Random Back-off time / Binary Exponential Back of.....16

ii. MILD.....17

2.1.3 SPECIALIZED MAC IN WIRELESS….....18

i. Hidden Terminal Problem.....19

ii. Exposed Terminal Problem 19

iii. Near Terminal 20

iv. Far Terminal ..……20

3 WIRELESS LOCAL AREA NETWORK.....21

3.1 INFRASTRUCTURE-BASED WLAN 21

3.1.1 MAC Algorithms in Infrastructure-based WLAN.....22

I. CSMA/CA.....22

3.2 INFRASTRUCTURE-LESS WLAN: “AD-HOC NETWORK” 23

3.3. Wireless Personal Area Network….....*24*

3.4. Wireless Cellular Network ……25
3.5. Wireless Sensor Network ……26

4 Medium Access Control……..26
4.1. OMNI-DIRECTIONAL ANTENNA MAC PROTOCOLS 27
i. CSMA/CA ..... ……27
ii. MACA / MACAW..... 28
iii. IEEE 802.11 MAC 29
iv. FAMA..... ……...30
v. DBTMA 31
4.2. Directional antenna MAC protocols ……31

5 Mobile ad-hoc network (MANET) Protocols……31
5.1. Proactive (Table-driven routing protocols) ……32
5.1.A. DSDV……33
5.2. Reactive or on-demand routing protocols*……..36*
5.2.A. DSR ……..37
5.2.B. TORA ……...42
5.3. Hybrid (Combination of Reactive & Proactive Protocols) ……43
5.3.A. AODV ……43.
5.4. Other routing protocols ……46

6 Methodology ……47
7. SIMULATION Environment ……..47

8. Performance Metrics……48
8.1 Packet Delivery Fraction (PDF) ……49
8.2 Throughput……49
8.3 Normalized routing load ……49

9. SIMULATION METRICS ……49
10. SIMULATION RESULTS……50
10.1 A. Throughput ……50
10.2 B. Routing load ……53
10.3 C. Packet Delivery Ratio……54

11. Congestion control in TCP……54
11.1 Comparison based on congestion control……55

12. NAM and XGRAPH……56
13. Comparison based on Bandwidth……57
14. Overall Performance Comparison……59
15. Conclusion ……60
16. Future Work ……60

LIST OF FIGURES

2.3.a: Collision at B due to Hidden Terminal Problem……19
2.3.b: Near and Far Terminals……20
3.1.a: Infrastructure-based WLAN having AP communicating with Wireless terminals and with wired LAN……..21
3.1.b: Stations accessing the medium using CSMA/CA……..23
3.2.a : Wireless Ad hoc Network……24
3.4.a : Cellular Network Architecture……..25
3.5.a: A Sensor Network……26
4.1.a: Complex hidden terminal problem……30
5.a: Classifications of mobile ad hoc routing protocols……32
5.2.A (i): Flooding of the route request to discover route record in DSR……..41
5.2.A (ii): Propagation of Route Reply in DSR……..41
5.3.A (i): Route request (RREQ) flooding ……46
5.3.A (ii): Route reply propagation……..46
10.1: Throughput vs. Packetsize……50
10.2: Throughput vs. Speed……51
10.3: Throughput vs. Time……52
10.4: Drop vs. Packetsize……52
10.5: Drop vs. Speed……52
10.6: Routing Load vs. Time……53
11.1, 11.2, 11.3: Comparison based on congestion control……56
12.1, 12.2, and 12.3: The relationship between nam file and xgraph……57
13.1, 13.2, and 13.3: Comparison between three routing protocols on the basis of Bandwidth vs. Time……59

1. INTRODUCTION

1.1. Wireless Communication

Wireless communication is the transfer of data from one place to another through electromagnetic waves. It is a mode of communication that uses free space instead of wires. Hence the data travels in the air as same as light does. Wireless communication mostly related to radio, microwave and infrared waves. Usually a wireless node has one antenna, for both sending and receiving. This makes collision detection difficult if not impossible. The problem does not go away even if the node has two antennas. The reason being that the sending signal has much higher power thus swamps any signal that might be coming in. There have been methods proposed in the literature [1, 2] to get over this problem by pausing while transmitting. Unfortunately even this approach does not enable a node to detect all kinds of collisions (even if we don't consider the overheads of this scheme in the low load case). The trouble is that collisions happen at the receiver and not the sender. Thus all the protocols we talk about in this paper don't even attempt collision detection. A common problem which has long been recognized in the wireless world is that of hidden terminal [3]. This problem occurs when two senders are not in the vicinity of each other (so cannot carrier sense each other's signals) but both of them are in the range of the common receiver. So carrier sensing fails in this case. The RTS/CTS exchange helps alleviate this problem to a certain extent (see below) but does not make it go away completely. A related issue is the exposed terminal problem, where a station can sense the medium busy because of a nearby sender and thus refrains from sending even when its transmission would not have collided at its destined receiver. This problem is not considered as serious as the hidden terminal problem and becomes irrelevant in case of protocols which acknowledgement at link layer (e.g. MACAW, DFWMAC) as in this case we cannot afford a collision even at the sender because of the incoming

acknowledgements. Another problem in similar vein as those above is that of capture. This occurs when the received power at the receiver from two senders is significantly different. The sender with higher power “captures" the receiver, which will never be able to sense the second signal. This leads to significant fairness problems. The wireless medium inherently has higher error rates because of interference between co-located LAN's, self-interference, fading, interference caused by other electronic devices and collisions. This needs to be taken into account in the protocol design phase. For instance, DFWMAC has link level acknowledgements to provide a better end-to-end service. A transceiver circuit has a turn around time, known as Rx/Tx-turnaround, to switch between receiving and transmitting. This imposes a restriction on how fast one can receive and respond back. Wireless protocols have to deal with this and it becomes a more serious issue when different transceivers are being used in the same LAN. For this reason there have been protocols proposed [4] that try to reduce the number of turnarounds. Power has always been a scarce resource in wireless devices. MAC protocols are expected to contribute towards efficient power utilizations. There have been very few solutions to this problem. The standards [5, 6] have not been able to deal with this effectively. The ability to support QoS is a difficult undertaking. This is not because of processing limitations like in the wired world, but because most of the protocols are contention based with no limits on how long the contention will last. Making these protocols contention free might sound like a solution but is not, because of low resource utilization achieved by these protocols. Also dealing with multiple hops in a potentially dynamic network is a hard problem. In spite of the fact the medium here inherently broadcast, the issues of multicast and broadcast has not been addressed by any MAC protocol [7]. Multicast functionality has eluded the wireless LAN at the MAC layer. The problem comes because of high error rates. In a large receiver set there are chances that one of the receivers will receive the packet in error. Also for obvious reasons acknowledgements cannot be used here for reliability (implosion effect). Because of this and other difficulties no MAC

protocol has come forward to supporting multicasting in wireless LAN's (multiple unicast based solutions are employed). Security becomes a bigger issue in wireless domain because of ease of snooping. Another problem area for wireless MAC protocols is dealing with high speed mobility. The system that enables wireless data communication is called the wireless network, e.g., radio channel network, TV network etc. It consists of either computer, laptops, notebooks, routers, switches, cell phones, portable phones, PDA's, related operating systems / software's, access points (AP), base stations (BS), antennas or towers etc. One network can interconnect with other network or sub network. As WLAN is one network but it can interconnects Bluetooth wireless system or can also support the wireless ad-hoc network. Furthermore, 2G and 3G cellular networks are running together, and they are adaptive to each other as well.

Importance: This type of communication is quite swift with a better output. Data can be exchanged in less time. People far away from each other can easily communicate at any time e.g., use of online chatting, cell phones, e-mails etc. It has many other advantages like to install the wireless system in a building will be easy comparative to fix all wires in the building for the wired network would be time taking, complicated and also headache.

1.2 Wireless Network

The system that enables wireless data communication is called the wireless network, e.g., radio channel network, TV network etc. It consists of either computers, laptops, notebooks, routers, switches, cell phones, portable phones, PDA's, related operating systems / software's, access points (AP), base stations (BS), antennas or towers etc. One network can interconnect with other network or sub network. As WLAN is one network but it can interconnects Bluetooth wireless system or can also support the wireless ad-hoc network. Furthermore, 2G and 3G cellular networks are running together, and they are adaptive to each other as well.

Types of Wireless network:

There are various types of wireless networks being used as; infrastructure-based WLAN, wireless Ad-hoc network, wireless personal area network (WPAN), wireless cellular network, satellite system, television network and wireless sensor network (WSN) etc. Each type of network uses slightly different techniques and algorithms from each other in all aspects including *MAC algorithms* as well. MAC plays vital role in wireless communication. There are currently two variations of mobile wireless networks, infrastructure and infrastructure less networks. Typical infrastructure networks are cellular mobile networks, which have fixed base stations, which are connected with other base stations through a wired backbone. The transmission range of a base station covers a cell. All the mobile nodes lying inside this cell connect to and communicate with the nearest base station. A "handoff" occurs when a mobile host travels out of range of one base station and into the range of another base station (change of cells).

The other type of network, infrastructure less network, is known as ad hoc network. These networks do not rely on an infrastructure and can operate without any base station or access point and without a backbone network. In mobile ad hoc networks, so called MANET, all nodes are capable of movement and can be connected dynamically in an arbitrary manner.

Wireless local area network (WLAN) is a fast-growing market in wireless domain. WLAN covers a limited geographical area as it is restricted within buildings, a campus or in a room etc. It can be divided into two groups according to their network configurations. First type of WLAN is infrastructure-based wireless network, and second is the infrastructure-less wireless network usually called *ad hoc* wireless network. There are 5 types of wireless network:

i. **Infrastructure based wireless network**
ii. **Infrastructure Less (ad hoc) wireless network**

iii. **Wireless personal area network**

iv. **Wireless cellular network**

v. **Wireless sensor network**

First type of WLAN is infrastructure-based wireless network, and
Second is the infrastructure-less wireless network usually called *ad hoc* wireless network. Each type of network uses slightly different techniques and algorithms from each other in all aspects including *MAC algorithms* as well.

2. Medium Access Control

Medium Access Control (MAC) algorithms are used to allow several users simultaneously to share a common medium of communication in order to gain maximum of channel utilization with minimum of interference and collisions. MAC is similar to traffic regulations in the highway. Several vehicles cross the same road at a time but rules required to avoid collision e.g., follow the traffic lights, building the flyovers etc. [9].

2.1 MAC Protocols

2.1.1 Basic MAC algorithms

Many MAC algorithms and protocols have been successfully used in wired networks for a long time. Some of them are quite famous and elegant algorithms such as ALOHA and *Carrier Sense Multiple Access* (CSMA). These are very basic schemes for multiple access channels, and they are also the basis for wireless channel allocation schemes. Therefore, we shall review them briefly in the following to develop better concepts for wireless MAC algorithms. There are two types of such algorithms;

I. Aloha
II. CSMA

- **Aloha**

In 1970s Norman Abramson proposed a new and reliable algorithm to solve the channel allocation problem in wired network. Abramson worked with his colleagues at the University of Hawaii to develop this method called ALOHA or Pure ALOHA. Its another version is called Slotted ALOHA [8].

Pure ALOHA is a random access protocol. A user can access the channel whenever it has data to be transmitted. Definitely, there will be a collision. However, after transmission the user waits for an acknowledgment from separate feedback channel. If there is collision, the sender waits for a random amount of time and retransmits the data. Pure ALOHA does not relate to time synchronization.

Slotted ALOHA divides the time into equal time slots of length greater than the packet duration. Each user has synchronized clock and transmits the data only at the beginning of new time slot. This helps in a discrete distribution of accessing the channel. But collision is not prevented absolutely; there is a collision with portions of data packets.

It is a very simple protocol in which a station sends data whenever it has data to send. The receipt of an acknowledgement (which might be implicit) assures the sender that data has been delivered successfully, else it is sent again after a random time gap. Aloha is useful in cases in which carrier sensing is not possible or impractical (like in satellite communications).

- **CSMA**

ALOHA does not listen to the channel before transmission. On the other hand, *carrier sense multiple access* (CSMA) algorithm is based on the concept that each station on the network is able to sense the channel before transmitting the data packet. Sensing the channel means to monitor the status of channel

whether it is idle or busy. If the channel is idle/free, then station can transmit the data. But if the channel is sensed busy, the station will wait and keep on sensing the carrier till it becomes free. This method decreases the probability of collision. There are several versions of CSMA exist:

Non-persistent: In this type of CSMA, a station senses the channel first. If the channel is free then it starts transmission immediately. But if channel is busy then the station does not continuously sense the channel, rather it waits for a random amount of time and then repeats the algorithm [9].

P-persistent: It is applied to slotted channel. Here stations also sense the medium. If the medium is free, a station transmits the packet with a probability of *p* or with probability of *1-p* if the station defers to next slot.

1-persistent: When a station wants to send the data, it first senses to the channel whether it is free or busy at the moment. If it is busy, the station waits until it becomes free. And if the station detects an idle channel, it transmits a data frame. When the channel becomes free the two or more neighboring stations can transmit data at the same time. This will cause collisions. If the collision occurs, the station waits a random amount of time and repeats the method. The algorithm is called 1-persistent because the station transmits with a probably of 1 whenever it finds an idle channel.

The fundamental reason for low channel utilization of Aloha protocol is that senders don't defer to each other even when another transmission is in progress. CSMA rectifies this problem by carrier sensing (explained above). If any node finds the medium busy in the network, it is supposed to get a random value within a **contention window** for back-off time. The node starts counting down its back-off time only when the medium becomes free.

2.1.2. BACK-OFF Algorithms

Thus, collision and loss of packets are the major problems in wireless networks compared to wired networks. Then how much time should be spent for waiting when the carrier is busy, waiting after collision or loss of packets etc. are other critical issues in wireless domain. However, some techniques and methods have also been applied besides the MAC algorithms to overcome these issues. The terminologies like *random amount of time / random back-off time* have been mentioned in ALOHA, CSMA and will be used in subsequent protocols too. The purpose of these techniques is to make a transparent and justified way of accessing the wireless medium. The real algorithms producing the random amount of time are the *Back-off Algorithms*. There are two types of such algorithms;

i. Random Back-off time/ Binary exponential back-off
ii. MILD

- **Random Back-off time/ Binary exponential back-off**

This is the mostly used algorithm in order to select the random amount for the duration of waiting time in the network. Here the random amount of time is the random back-off time that counts downwards to zero. This time delays the access of medium in order to provide transparent and collision free environment for all nodes in the network. Whenever, if any node finds the medium busy in the network, it is supposed to get a random value within a **contention window** for back-off time. The node starts counting down its back-off time only when the medium becomes free. Each node may have different or same amount of time but within contention window. This random waiting time avoids collisions; otherwise all nodes would have accessed the idle medium at the same time. After finishing that random time, they start sensing the medium. As soon as a node senses the channel is busy, it loses this turn and it will select another back-

off time for the next cycle. On the other hand, if a node gets the medium free after waiting for random time, it can access the medium immediately [9]. Contention window (CW) is set with an initial size e.g. 7 min = *CW* . The back-off time is selected from the CW and it could be any value between 1 and 7. CW becomes double + 1 at each time for every collision or lost frame. The window can take on the values 7, 15, 31, 63, 127, 255 and so on. Let maximum size of CW in this example is 255 max = *CW*. The collision indicates the load on the network, and then doubling the value of CW can minimize the chances of collision. It is hard to select the same random back-off time using large CW. This algorithm is also called the *Binary Exponential Back-off* (**BEB**), because CW doubles (having linear graph) at each time of collision [1]. The value of CW is reset to its original minimum value (CW=7) as soon as any transmission completes successfully after the occurrence of collision. The standard size of CW in **802.11a**: 15 min = *CW* 1023 max = *CW*, and in **802.11b**: 31 min = *CW* 1023 max = *CW*.

Collision and loss of packets are the major problems in wireless networks compared to wired networks. Then how much time should be spent for waiting when the carrier is busy, waiting after collision or loss of packets etc. are other critical issues in wireless domain.

- **MILD**

The MILD stands for *multiplicative increase and linear decrease*. The contention window (CW) is also set in this algorithm. Initially a minimum value is selected for CW, say CW = 5. At each time of collision, instead of doubling the CW, here the CW is increased by multiplicative factor; say 1.5. Thus, CW would become 5x1.5 = 7.5, at first collision. Moreover, at the time of successful transmission after collision the CW is linearly decreased; let's assume by 1. So, it would be 7.5 – 1 = 6.5 [5].

2.1.3. Specialized MAC in wireless

The main question is why elaborated schemes used in wired network are fail in wireless world. This is due to several effects that occur only in wireless network. To explain in detail, let us consider first **Carrier Sense Multiple Access with Collision Detection** (CSMA/CD), one of the MAC schemes being used in wired networks. **CSMA/CD** works as follows: A sender A wants to transmit data to a receiver B. Then A senses the medium (wire or coaxial cable) to check that the medium is free or not. If it is busy, the A waits until it becomes free. But if the medium is free, the A starts transmitting data and continues to listen into the medium. If sender A detects a collision while sending data, it stops at once and sends a jamming signal [10]. CSMA/CD aims that the signal should reach the receiver without collisions. The sender is the one detecting collisions. This is not a problem using wire, as more or less the signal strength remains same all over it. If collision occurs somewhere in the wire, everybody notices that. It is not the case that a sender listens into the medium only to detect the collision at its own location, rather in reality is trying to detect a possible collision at the receiver side [9]. Why does this scheme fail on wireless networks? The situation is different in wireless networks. As there are no wires and the signal propagates in more than one direction and faces resistance from walls, trees and other things etc. This implies, "*the strength of a signal decreases proportionally to the square of the distance to the sender"*. Let's apply CSMA/CD here. The sender senses the medium and finds it idle. It starts sending but a collision occurs at the receiver due to the second sender. It is because of hidden terminal problem [9]. Collision detection is very difficult in wireless scenarios as there is no physical connection between stations. Also the transmission and detection range is limited, and thus data transmissions of various stations cannot be detected every time. All critical problems which are the reasons for special MACs required in wireless networks explained below:

i. Hidden Terminal Problem

Consider the situation as shown in the **Figure 2.3.a.** There are three mobile phones A, B and C. The transmission and detection range of A reaches B, but not C. The same applies to C. The transmission and detection range of C reaches B, but not A. Hence A cannot detect C and C cannot A either. That means A is ***hidden*** for C and vice versa. The transmission range of B reaches both A and C. A starts sending to B, C does not receive this transmission. At the same time C also wants to send something to B and senses the medium. The medium appears to be free, thus the carrier sense fails. C now starts sending and causes a collision at B. The both senders A and C cannot detect this collision at B and will keep on sending. Also, both will assume that the data has been transmitted without errors, but actually the collision has destroyed the data at the receiver. This is only due to hidden problem as A and C both are hidden to each other.

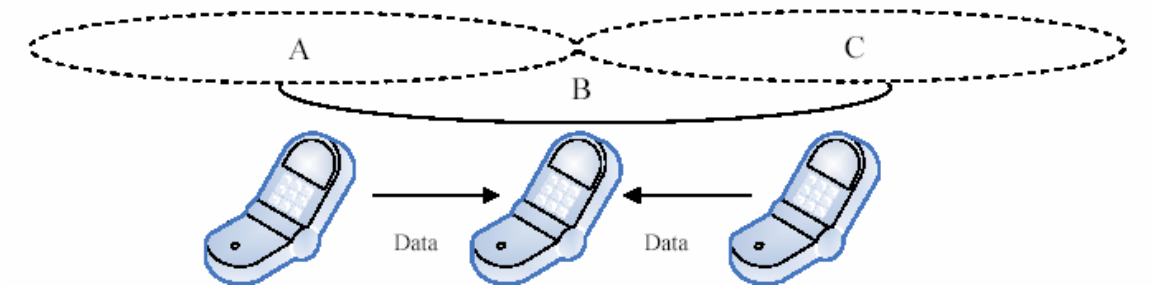


Figure 2.3.a: Collision at B due to Hidden Terminal Problem

ii. Exposed Terminal Problem

This effect does not destroy data, but causes only unnecessary delays. Consider the same scenario shown in **Figure 2.3.a**. Now B sends something to A. Simultaneously C wants to transmit data to some other mobile phone outside the interference ranges of A and B. C senses the carrier and detects that the carrier is busy just because of B's signal. It will postpone its transmission until it detects the medium becomes idle. But A is outside the range of C, so waiting is not

required. The collision that would have occurred at B does not matter, because it is too weak to propagate to A. So C is exposed to B.

iii. Near Terminal

The situation in **Figure 2.3.b** shows three mobile phones, where A and B are both sending to C with the same transmission power. Consider C as a base station (BS). As the strength of a signal decreases proportionally to the square of the distance, B's signal drowns out A's signal because B is near to BS. As a result, C cannot receive A's transmission [9].

iv. Far Terminal

Now C has to send signals to both terminals A and B. As B is quite near to BS, it will receive the transmission clearly. But A is far enough from C that it would not be able to get fair transmission. Hence stations that far away are badly affected by the near terminals and other resistance like free space loss, reflection etc.

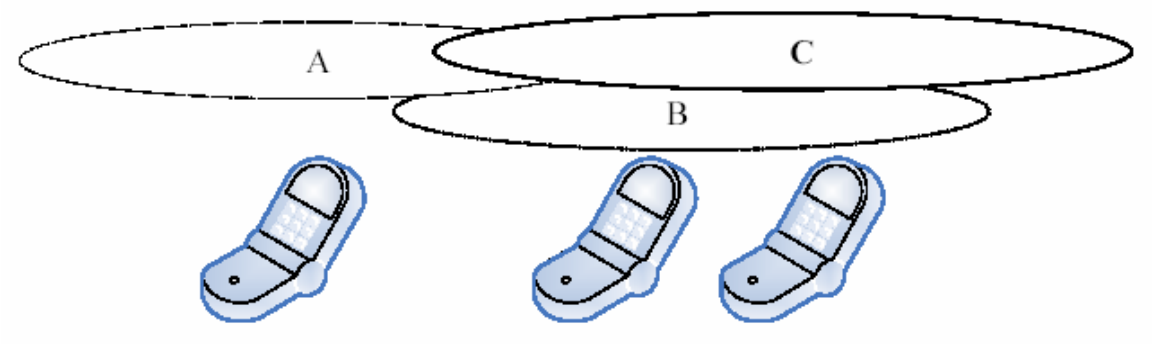


Figure 2.3.b: Near and Far Terminals

3. Wireless Local Area Network

Wireless local area network (WLAN) is a fast-growing market in wireless domain. WLAN covers a limited geographical area as it is restricted within buildings, a campus or in a room etc. It can be divided into two groups according to their network configurations. First type of WLAN is infrastructure-based wireless network, and second is the infrastructure-less wireless network usually called *ad hoc* wireless network.

3.1. Infrastructure based wireless network:

In Infrastructure-based networks, communication can take place only between an access point (AP) and the wireless terminals. There is no direct communication between wireless terminals; usually called nodes or stations. AP does not control just wireless medium, but it also acts as a bridge to other wireless or wired networks.

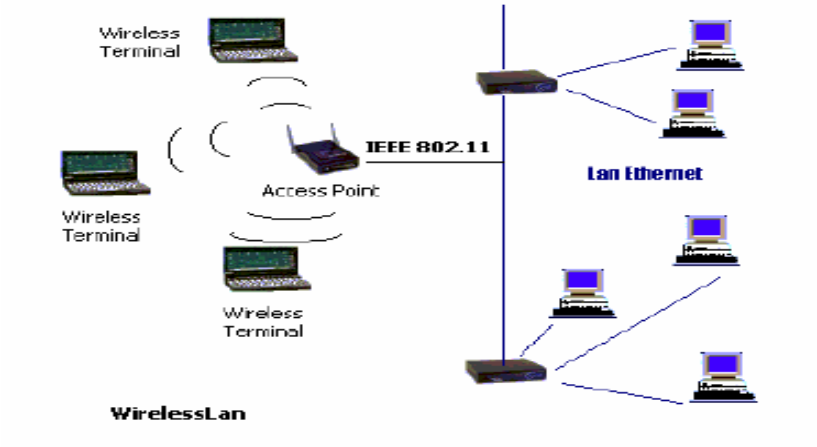


Figure 3.1.a: Infrastructure-based WLAN having AP communicating with Wireless terminals and with wired LAN

This type of network uses many medium access schemes. These schemes mostly based on carrier sensing and virtual sensing, trying to reduce collisions, provide fair medium access by using back-off algorithms and avoiding hidden and exposed terminal problems.

3.1.1. MAC Algorithms in Infrastructure-based WLAN

Variety of medium access methods and techniques has been designed for WLAN. Many of them have been deployed successfully. New methods are still being proposed in the market. The paper is going to narrate some of the MAC methods which have been implemented successfully for the commercial use.

i. CSMA/CA

The basic CSMA scheme has come up with the concept of *collision avoidance* by using *random back-off time*. So, the CSMA/CA introduces the BEB algorithm in order to create some fairness for waiting time and importantly to reduce the probability of collisions. In the very first cycle, if a station finds the channel free starts its transmission immediately. Consider the scenario in Figure 3.1.b, the station B gets free medium in first cycle and hence starts transmission. All other stations A, C and D got the busy channel in first cycle, they now select the random back-off time each within a contention window (CW). In the beginning of next cycle, the stations A, C and D want to send data and start sensing the medium. As soon as stations sense the idle medium, they begin to counting their back-off times. The station D had small back-off time, D finishes it very early and gets the free medium and thus starts transmission. But other two stations A and C continued with back-off time, and after finishing their times they got a busy medium. Now A and C will wait for next cycle having new back-off time and repeat the whole algorithm again. Moreover, if two stations finish their back-off times simultaneously, they will start their transmission together provided the medium is idle, and hence there will be a collision. The collision triggers a new value of contention window (double+1). As soon as the receiver gets the packet and it answers with an acknowledgment packet ACK. The ACK confirms the correct reception of data. If no ACK is received by sender, it will retransmit the packet in future. But the sender has to follow the whole algorithm again to access the channel. No special rule has been designed yet for retransmission.

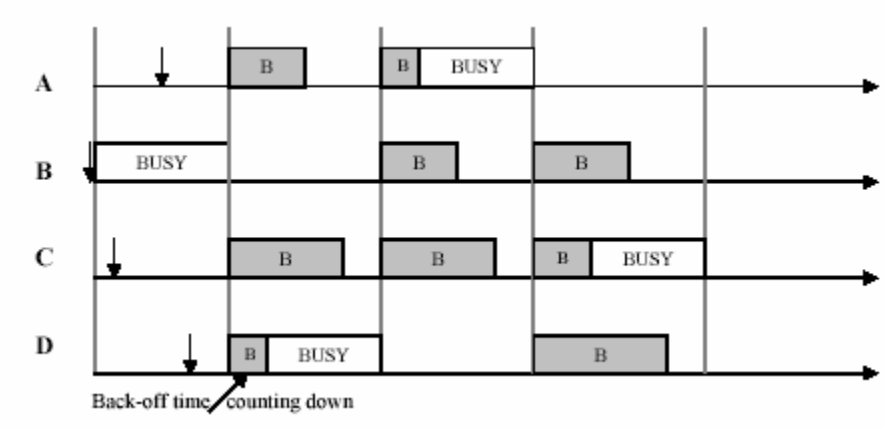


Figure 3.1.b: Stations accessing the medium using CSMA/CA

3.2. Infrastructure Less (ad hoc) wireless network

As to infrastructure less approach, the mobile wireless network is commonly known as a mobile ad- hoc network (MANET) [16, 17]. A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly. Wireless ad hoc networks themselves are an independent, wide area of research and applications, instead of being only just a complement of the cellular system. Ad-hoc network doesn't need any base stations. Each node work as a router and services are not required.

A mobile ad hoc network (MANET) is a wireless network temporarily and dynamically created only by mobile stations (MSs) without using any pre-existing infrastructure. Means there is no base stations or access points like in infrastructure-based WLAN. The Figure 3.2.a. is showing that all stations communicating with each other without an AP. A MS (laptop, mobile phone, PDA) in this system performs all tasks like access point, router and including its own applications etc. A MS could be in moving state while in ad-hoc network and

it can join or disjoin the network any time at its own will. So there is no fix topology. Hence the multiple hops communication exists among the nodes. Each node has a responsibility of relaying packets for others and a packet has to traverse multiple nodes to reach a destination. Such unique features make ad hoc networks distinct from other types of wireless networks.

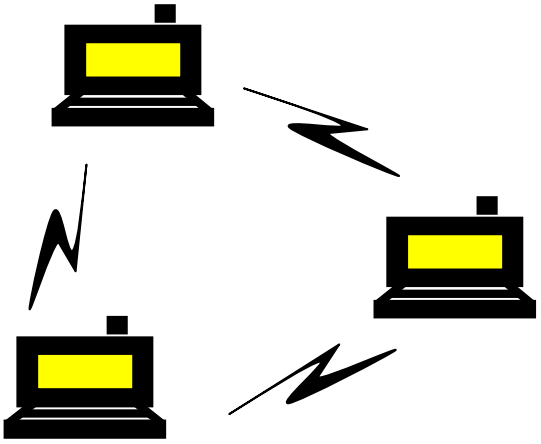


Figure 3.2.a : Wireless Ad hoc Network

3.3. Wireless Personal Area Network

The IEEE 802.15 is the standard for Wireless Personal Area Networks (WPANs). It was formed to develop standards for short range wireless devices separated by up to 10 meters, unlike WLAN where devices could be separated by up to 100 meters, and the cellular network that spans over the range of 100 of kilometers. Devices in a PAN may include portable and mobile computers (laptops), cell phones, pagers and other mobile devices. The WPAN is a form of ad hoc network. The notion of IEEE 802.15 was originally created by the *Bluetooth* technology in 1999.

3.4. Wireless Cellular Network

There has been a tremendous growth in wireless cellular technology over the last decade. The term *cellular* refers that the certain geographical area is divided into small areas called **cells**. Each cell contains a **base station** (BS). The BS transmits and receives the signals to and from the **mobile stations** (MS) in its cell. The coverage area of a cell depends on transmitting power of BS, the transmitting power of MS, buildings and mountains in a cell etc. Each base station is connected to **mobile switching center** (MSC) as shown in the Figure 3.4.a. The MSC is then connected to Public Switched Telephone Network (PSTN) which serves the functionalities as done by conventional telephone switching center [11].

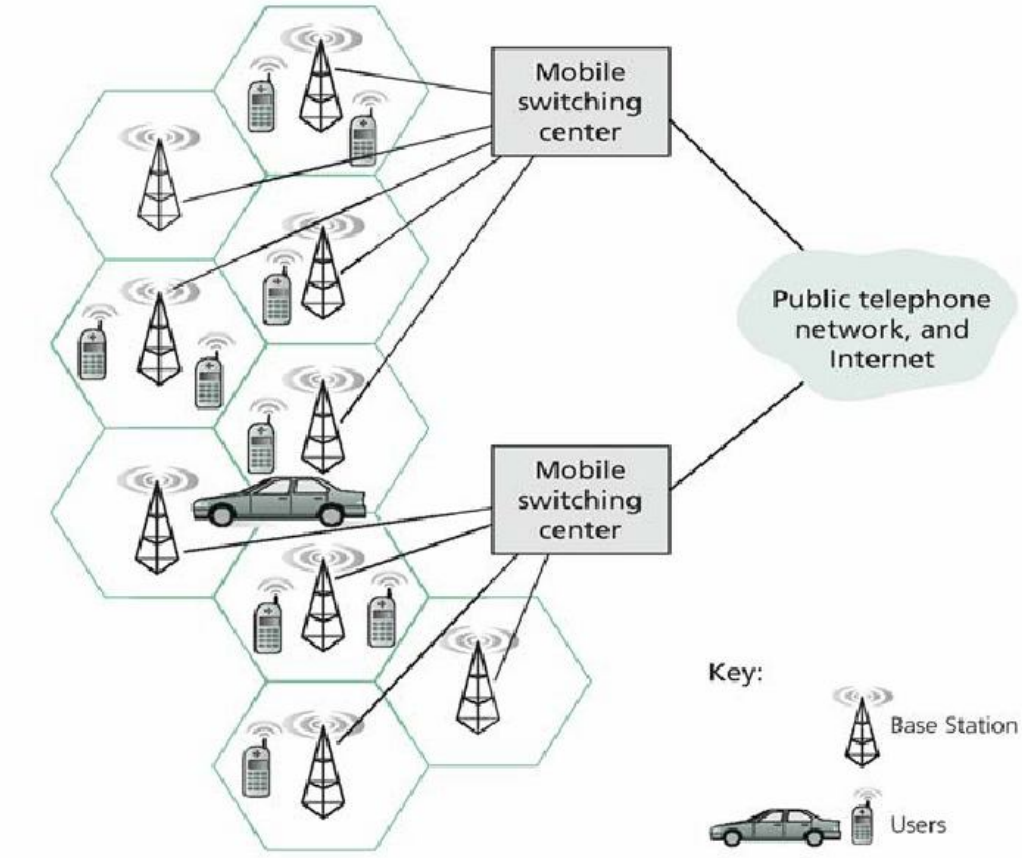


Figure 3.4.a : Cellular Network Architecture

3.5. Wireless Sensor Network

A wireless sensor network (WSN) consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and certain level of intelligence for signal processing and communication of the data. WSNs are becoming more functioning as they are used in military to detect and gain information about enemy movements, explosions etc., wireless traffic sensor networks to monitor vehicle traffic on highways, security system using sensors for target detection and tracking and also used in tactile system, ubiquitous computing etc. Specifically in WSNs, nodes coordinate locally to perform data processing and deliver messages to a common sink or cluster.

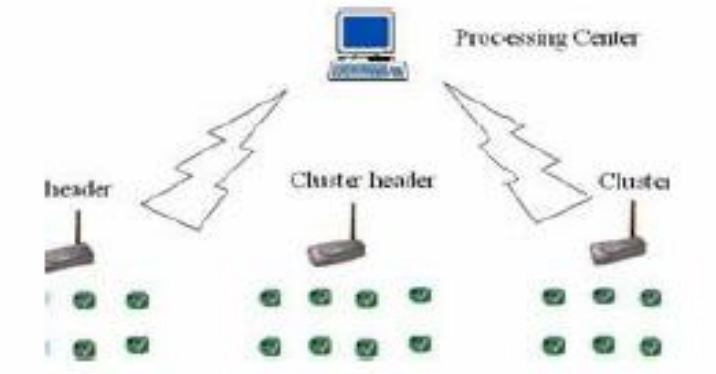


Figure 3.5.a: A Sensor Network

4. Medium Access Control

Medium Access Control (MAC) algorithms are used to allow several users simultaneously to share a common medium of communication in order to gain maximum of channel utilization with minimum of interference and collisions. MAC is similar to traffic regulations in the highway. Several vehicles cross the same road at a time but rules required to avoid collision e.g., follow the traffic lights, building the flyovers etc. [9].MAC belongs to layer 2; the Data Link Control layer (DLC) of the ISO *OSI reference model*. Layer 2 is subdivided into the MAC layer 2a, and logical link control (LLC) layer 2b. The task of DLC is to establish a reliable point-to-point or point–to-multipoint connection between different devices over wired or wireless medium.

MAC algorithm in ad-hoc network

4.1. Omni directional antenna MAC protocols

- **CSMA/CA:**

Carrier senses multiple accesses with collision avoidance (CSMA/CA) is one of the earliest multiple access schemes adopted for ad hoc networks after its success in infrastructure based WLAN. CSMA attempts to avoid collisions by sensing carrier in the vicinity of the transmitter. Collisions however occur at the receivers, not at the transmitter. In an ad-hoc wireless network the performance of CSMA/CA is still limited by the so called hidden and exposed terminals. The scheme has been explained well in section 3.1.1. Thus CSMA does not provide an appropriate mechanism for collision avoidance.

Issues: The well known CSMA/CA is one of the basic medium access algorithms used in wireless networks. Ad-hoc networks also adopted it in very early times. But the major issues of hidden terminal and exposed terminal problems are exist in this area as well. Due to this it does not provide satisfactory results. In addition, CSMA/CA does not support access on priority bases in ad-hoc wireless networks.

- **MACA**

MACA (multiple access collision avoidance) was the first modern protocol which used RTS/CTS exchange and underscored the benefit of it over the then existing protocols (which were largely CSMA/CA based). The motivation was again the hidden terminal problem. In MACA before a station sends the data it sends an RTS message to the receiver. On success the receiver responds with CTS. The nearby stations are also listening to this exchange. If a station hears RTS it waits for the corresponding CTS. If it does not hear CTS, it means any transmission it has will not interfere with the receiver. The assumption here is if you cannot hear the receiver, the receiver cannot hear you too. This helps alleviate the exposed terminal problem. Any station, other than the original RTS sender, on hearing

CTS will defer its transmission. The time for which to defer transmission depends on the packet length to be transmitted which is contained in the CTS packet. This takes care of the hidden terminal problem. Binary exponential backoff was used in case of collisions of RTS packets. MACA requires much simpler hardware because of absence of carrier sense.

- **MACAW**

Various practical problems with MACA were identified by MACAW (MACA for Wireless) [12] and proposed changes that solves some of them. This was one of the first wireless MAC protocols that were designed with fairness in mind. MACAW gets rid of Ethernet like unfairness associated with binary exponential backoff algorithms by proposing a copying form of backoff counter in which nodes use the backoff counter of a successful transmission to contend fairly in the next cycle. Also separate backoff parameters were introduced (corresponding to different streams) to avoid this copied parameter to spread widely even to areas with no congestion. It also proposed a multiple stream model for fairness among streams emerging from the same station. MACAW acknowledged the importance of link layer acknowledgements and made the protocol from RTS-CTS-Data to RTS-CTS-Data-ACK. With the introduction of this ACK packet means that exposed terminals should not transmit now, or else they will trash the incoming ack. There are two ways of dealing with this, carrier sense or an explicit packet specifying the length of the transmission at the start of it. MACAW takes the latter approach to keep the hardware simple and calls this packet DS (data sending). Another control packet RRTS (Request for RTS) was added to let the receiver contend for the sender to improve fairness in cases when there are two receivers in the vicinity of each other (thus only one can receive). By making the protocol significantly more complex MACAW lost performance when the channel was lightly loaded but led to much better throughput and fairer allocation in presence of high loads.

- **IEEE 802.11 MAC**

The IEEE works here as well by introducing IEEE standard 802.11 for WLAN. The standard's number indicating that it belongs to the group of 802.x LAN standards, e.g., 802.3 for Ethernet and 802.5 for Token Ring etc. Therefore, this standard IEEE 802.11 focuses only on physical (PHY) and medium access control (MAC) layers. Basically MAC layer provides the mandatory asynchronous data service and an optional time bounded service. The 802.11 MAC offers both types of services for infrastructure-based WLAN, while it offers only asynchronous data service for ad-hoc network mode. The three different access mechanisms have been defined for IEEE 802.11 MAC; first one is based on CSMA/CA, second is on MACA/MACAW, and the last one is the Polling method. The first two methods can also be categorized as *distributed coordination function* (DCF), it offers only asynchronous data service. The third method can be called *point coordination function* (PCF) and it offers both asynchronous and time-bounded service. The IEEE 802.11 MAC schemes are also called *distributed foundation wireless medium access control* (DFWMAC) [9]. The unique feature of 802.11 MAC is the fix parameters for waiting time before accessing the medium. This waiting time is other than the back-off time. There are three different types of parameters. They define the priorities of medium access.

DCF inter-frame spacing (DIFS): Any node in the network if finds the medium free for the transmission, it has to wait first for duration of DIFS. This parameter has longest waiting time and has lowest priority of medium access.

Short inter-frame spacing (SIFS): It is the shortest waiting time for medium access and used before sending the ACK or polling responses. It has highest priority being shortest waiting time.

PCF inter-frame spacing (PIFS): This waiting time is used in polling method. An access point has to wait PIFS before accessing the medium. This waiting time is between DIFS and SIFS, and obviously has medium priority [1].

- **FAMA**

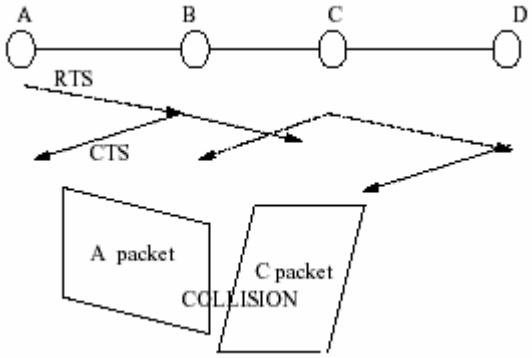


Figure 4.1.a: Complex hidden terminal problem

On first thought MACA seems to solve the hidden terminal problem, but that's not quite true. This happens primarily because the neighbors may not be able to hear CTS/RTS messages correctly. For example consider the topology in figure 4.1.a in which only adjacent nodes can hear each other.

A completes a successful RTS-CTS exchange with B and starts transmitting data. C which is a neighbor of B also started a RTS sequence just at the time B replied CTS to A, and hence is not able to realize that B is going to be in conservation. (B's CTS, C's RTS collide at C). D sends a CTS signal to C and C now thinks he has acquired the channel and starts transmitting the data which collides at B. One solution to this problem would be to make the length of CTS packet longer then the RTS packet, which would make sure that C hears the B's CTS message. This is only one instance in which the protocol fails and one can easily come up with other scenarios where it fails. Floor acquisition multiple accesses, FAMA, [13] represents a family of MAC protocols which operate in two phases, acquire the channel (floor acquisition) followed by the actual

transmission of data. These protocols ensure that data packets will be collision free and multiple packets can be sent by the sender. A key distinguishing observation is that this guarantees once channel is successfully acquired transmission of data packets is collision free unlike in MACA (or MACAW), where even after a successful RTS-CTS exchange, data packets can collide with other nearby transmissions (like above). FAMA has various variants each having different timing requirements for floor acquisition and performance characteristics. The variants are based on techniques used to acquire the floor and scope of the problem addressed (like single hop vs ad hoc networks). For example [14] authors prove that sending RTS packets without sensing the medium is inherently inefficient than using non persistent CSMA based techniques. An important and novel contribution of the work is derivation of sufficient timing requirements that must be met for correctness based on propagation delay, packet sizes, RTS/CTS sending timings, and Rx/Tx-turnarounds.

- **DBTMA**

Dual Busy Tone Multiple Access (DBTMA) distinguishes itself from other MAC protocols in two aspects: it splits a single channel into two sub-channels, and secondly it uses a pair of transmitting and receiving busy tones to serve the virtual sensing [15].

4.2. Directional antenna MAC protocols

- MAC/DA1
- MAC/DA2
- DBTMA/DA

5. Mobile ad-hoc network (MANET) Protocols

Mobile ad hoc networks can be classified into two main categories:

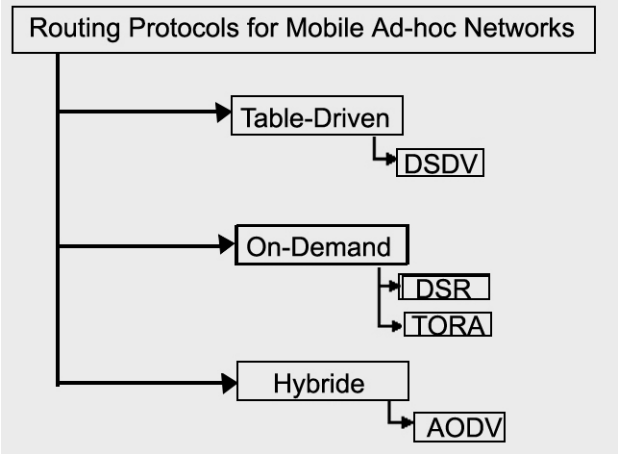


Fig. 5.a: Classifications of mobile ad hoc routing protocols.

5.1. Proactive (Table-driven routing protocols)

Proactive routing protocols use periodic broadcasts to establish routes and maintain them. They try to maintain complete routes from each source in the network to all other nodes. Proactive protocols are, in general, derived from the distance vector and link-state schemes of the wired network protocols**.** Proactive routing protocols use periodic broadcasts to establish routes and maintain them. Since they exchange topology information enabling each node to maintain an up-to-date view of the network, proactive protocols are also called **table-driven protocols**. They try to maintain complete routes from each source in the network to all other nodes. This information is generally cached in tabular form with one or more tables being used by the different protocols. In order to maintain a consistent view of the network at each node, the protocols continuously propagate updates of topological changes throughout the network. Example is Destination-Sequenced Distance Vector routing protocol (DSDV).

Proactive protocols can effectively route packets immediately to any other node in the network and do not suffer from a high starting latency. They have been adapted and modified to solve the problems that the static network protocols faced in the dynamic mobile ad-hoc environment.

However, the periodic topology exchange results in a larger overhead especially when node mobility is high. Pro-active protocols, in order to maintain the constantly changing network graph due to new, moving or failing nodes, require continuous updates, which may consume large amounts of bandwidth. Even worse so much of the accumulated routing information is never used, since routes may exist only for very limited periods of time.

- DSDV (Destination-Sequenced Distance Vector routing protocol)

5.1. A. DSDV

Destination Sequenced Distance Vector (DSDV) is a Proactive routing protocol that solves the major problem associated with the Distance Vector routing of wired networks i.e., Count-to-infinity, by using Destination sequence numbers. Destination sequence number is the sequence number as originally stamped by the destination. The DSDV protocol requires each mobile station to advertise, to each of its current neighbours, its own routing table (for instance, by broadcasting its entries). The entries in this list may change fairly dynamically over time, so the advertisement must be made often enough to ensure that every mobile computer can almost always locate every other mobile computer. In addition, each mobile computer agrees to relay data packets to other computers upon request. At all instants, the DSDV protocol guarantees loop-free paths to each destination.

Routes with more recent sequence numbers are always preferred as the basis for making forwarding decisions, but not necessarily advertised. Of the paths with the same sequence number, those with the smallest metric will be used.

The routing updates are sent in two ways: a “full dump” or incremental update. A full dump sends the full routing table to the neighbours and could span many packets whereas, in an incremental update only those entries from the routing

table are sent that has a metric change since the last update and it must fit in a packet. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast changing network, incremental packets can grow big, so full dumps will be more frequent.

The updates can be time triggered (periodic) or event triggered. When any new or substantially modified route information is received by a Mobile Host, the new information will be retransmitted soon (subject to constraints imposed for damping route fluctuations). When a stabilized route shows a different metric for some destination that would likely constitute a significant change that needed to be advertised after stabilization. If a new sequence number for a route is received, but the metric stays the same, that would be unlikely to be considered as a significant change. Newly recorded routes are scheduled for immediate advertisement to the current Mobile Host's neighbours. Routes which show an improved metric are scheduled for advertisement at a time which depends on the average settling time for routes to the particular destination under consideration.

A broken link is described by a metric of infinity (i.e., any value greater than the maximum allowed metric). When a link to a next hop has broken, any route through that next hop is immediately assigned infinity metric and assigned an updated sequence number. Since this qualifies as a substantial route change, such modified routes are immediately disclosed in a broadcast routing information packet. The Destination Sequenced Distance Vector (DSDV) routing algorithm is the modification of the classic Distributed Bellman-Ford (DBF) algorithm. In a MANET any node in the network may be required to act as router and so each node maintains a routing table that lists all the nodes in the network of which it is aware. Each entry in the table contains the destination and the next hop addresses as well as the cost (in terms of hops) to get to the destination. The reason DSDV is an improvement on the original wired network protocol is that it avoids DBF's tendency to create routing loops. Each entry in the routing

table and a protocol message update is marked with a sequence number. This number is maintained by the destination node of a route entry and is increased whenever the node publishes its routing information. The sequence number value is used by all other nodes in the network to determine the “freshness” of the information contained in a route update for the destination. Since the value is sequentially incremented, a higher sequence number implies that the routing information is newer.

In order to maintain routing information consistency in the network each router shares its routing table with its neighbors by means of routing updates. These updates are done both in a periodic and triggered fashion. The designers of the protocol proposed this method with the aim of alleviating the potentially large amount of network traffic that will be induced by the routing updates. In a periodic update which occurs at predetermined regular intervals, a node broadcasts its entire routing table in a packet termed a full dump. Incremental routing update packets are used when triggered significant topological change. The change could be either due to node mobility or link breakages to next hop neighbors. The incremental update packets only contain those entries which have changed since the last periodic update. The triggered updates with the smaller packet sizes result and in the reduced overhead incurred by the protocol. A route table update entry contains the destination address of a node, the cost to reach it and the highest known sequence number for the destination. When a node receives an entry for a particular destination with a higher sequence number its old entry is replaced with the newer route. In the case where a node has to choose between two entries with the same sequence number, it selects the path with the least cost. An intermediate node that detects a broken route to a destination assigns an infinity value to the route’s path cost, increments the entry destination sequence number and immediately broadcasts the information as an update. Using this technique critical network topology information such as link breakages is disseminated quickly across the network.

Advantages and Disadvantages

The main advantage of DSDV over traditional distance vector routing protocols is that it guarantees loop freedom.

The protocol has a number of drawbacks. Optimal values for the parameters like maximum settling time for a particular destination are difficult to determine. This might lead to route fluctuations and spurious advertisements resulting in waste of bandwidth. DSDV uses both periodic and triggered routing updates, which could also cause excessive communication overhead. In addition, in DSDV a node has to wait until it receives the next route update originated by the destination before it can update its routing table entry for that destination. Finally, DSDV does not support multi-path routing.

5.2. Reactive or on-demand routing protocols:

Reactive routing schemes only become active after there is a request for a route. Reactive routing protocols have also coined the term on-demand protocols since these routing schemes create and maintain routes only when such routers are in demand. That's why it is also called as the **Source Initiated on Demand Routing protocols.** There is no periodic update of routing information between the nodes in the network with reactive protocols and so it is most often the case that a requested route is not known a priori. When required a node in the network requiring a route has to perform some type of route discovery to find a suitable route. Once a route is found, the node can begin transmission of data packets towards the intended destination. If the conditions in the network remain similar to the instant the route discovery process created the route, the route can be used without disruption as long as it is needed. If however conditions do change, due to link breakages or mobility, the source node has to repair the route or re-create it. Thus reactive routing protocols, in general, have a two phase operation: a route discovery phase and a route maintenance phase. Some well-known

reactive protocols are Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA) etc.

The motivation in the design of this ad-hoc routing philosophy is to reduce the protocol routing overhead created by periodic updates of the table-driven schemes. The proactive schemes also use significant resources to maintain certain routes which have the possibility of never being used. This is avoided by the reactive schemes which only create and maintain routes when they are needed.

Reactive (On-demand) protocols cause delays since the routes are not already available. Additionally, the flooding of the network may lead to additional control traffic, again putting strain on the limited bandwidth.

- DSR
- TORA

5.2. A. DSR

Dynamic Source Routing (DSR) is a reactive protocol i.e. it doesn't use periodic advertisements. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.

There are two significant stages in working of DSR: Route Discovery and Route Maintenance. A host initiating a route discovery broadcasts a *route request* packet which may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the *target* of the route discovery, for which the route is requested. If the route discovery is

successful the initiating host receives a *route reply* packet listing a sequence of network hops through which it may reach the target. In addition to the address of the original initiator of the request and the target of the request, each route request packet contains a *route recor*d, in which is accumulated a record of the sequence of hops taken by the route request packet as it is propagated through the network during this route discovery.

While a host is using any source route, it monitors the continued correct operation of that route. This monitoring of the correct operation of a route in use is called *route maintenanc*e. When route maintenance detects a problem with a route in use, route discovery may be used again to discover a new, correct route to the destination.

To optimize route discovery process, DSR uses cache memory efficiently. Suppose a host receives a route request packet for which it is not the target and is not already listed in the route record in the packet, and for which the pair (initiator address, request id) is not found in its list of recently seen requests; if the host has a route cache entry for the target of the request, it may append this cached route to the accumulated route record in the packet, and may return this route in a route reply packet to the initiator without propagating (re-broadcasting) the route request. The delay for route discovery and the total number of packets transmitted can be reduced by allowing data to be piggybacked on route request packets. DSR uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead, particularly during periods when little or no significant host movement is taking place. DSR has a unique advantage by virtue of source routing. As the route is part of the packet itself, routing loops, either short-lived or long-lived, cannot be formed as they can be immediately detected and eliminated.

This is a simple and self containing protocol that is used in MANET. In this case the entire packet contains the detailed information about the routing path. So no extra processing is required in the middle nodes of the path. More over no administrative things are also not required. This will happen only when a path is required to establish. Since each knows the details of the total view of the networking, it finds the suitable path and adds this path to the packets that are being sent.

Whenever a node changes it's position it is broadcasted to the all possible node describing how many "hops" are required to reach it.

"The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use."

The Dynamic Source Routing (DSR) protocol is based on the concept of source routing in which a source node determines the complete sequence of nodes through which to forward data packets. A node sending a packet to a destination node explicitly lists the route to the destination in the header of the packet. The list identifies each "next hop" node that should be taken in order to get from the source to the destination. Each node in the network maintains a route cache that contains source routes that the node is aware of. The route cache is continually updated with old unused routes being purged and new routes inserted as a node learns about them.

Characteristic of an on-demand algorithm DSR has two procedures: route discovery and route maintenance. When a node requires a route to a destination its first action is to consult its route cache to determine if it already contains a

route to the destination. If an unexpired route is found, the route is used for data transmission. However, if there is no route in the nodes cache, it initiates a route discovery process by generating and broadcasting a route request (RREQ) packet across the network. The RREQ packet contains the IP addresses of the source and destination nodes, a unique route request ID and a route record which will contain the addresses of the sequence of nodes for the route. To limit the number of route requests traversing the network, each node only processes a route request once. The source nodes address and the unique route request ID are temporarily cached and if the node receives another request with the same details it silently drops the packet.

When an intermediate node (any node other than the source and destination) receives a route request that it can process, its first action is to determine if its address is in the packet's route record. If the route record already contains the nodes address a routing loop has occurred and the packet is dropped. If there is no routing loop, the intermediate node inspects its route cache for an unexpired route to the destination. It generates and sends a route reply (RREP) packet to the source node if such a route is found. If a route is not found in the route cache, the intermediate node adds its own address to the route record in the RREQ and broadcasts it to its neighbors. The route request packet is thus flooded in the network until either an intermediate node or the destination node itself replies to it. This process is shown in Figure 5.2.A (i). Note that the replying node, given a choice between two routes, chooses the route with the least hop count. The route reply packet is routed back to the source node by reversing the order of the next hops in the route record of the original route request packet. The route reply that is sent back to the source node with the route record included. This can be seen in Figure 5.2.A (ii).

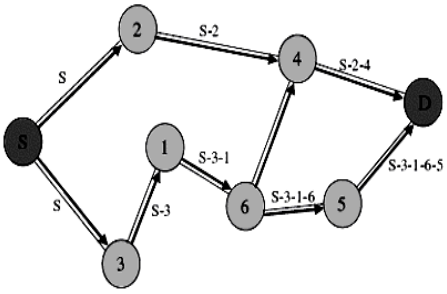


Figure 5.2.A (i): Flooding of the route request to discover route record in DSR

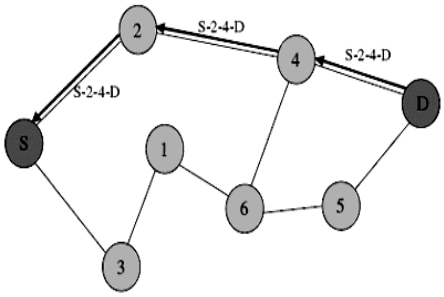


Figure 5.2.A (ii): Propagation of Route Reply in DSR

The route maintenance procedure of the protocol monitors the operation of a route and is responsible for making the source node aware of any errors. If an intermediate node detects a failure to transmit a data packet to a downstream link it generates a route error (RERR) packet. When a route error is received by a node, the node in the route error is removed from the nodes route cache and all routes containing that node are truncated at that point. Link errors are detected by means of link layer feedback and/or data acknowledgements.

One of the many optimizations proposed for DSR is the operation of the protocol in a “promiscuous” mode. In this mode the network protocol receives all packets (RREQ, RREP, and RERR) that the node’s wireless interface overhears. These packets are studied for useful source routes or route error messages after which they are discarded.

Advantages and Disadvantages

The major advantage of DSR is that there is little or no routing overhead when a single or few sources communicate with infrequently accessed destinations. In such situation, it does not make sense to maintain routes from all sources to such destinations. In DSR, only the sources that desire communication with such destinations need to discover those routes. Furthermore, since communication is

assumed to be infrequent, a lot of topological changes may occur without triggering new route discoveries (i.e. has little or no communication overhead).

There are a few drawbacks to the operation of DSR. Even though DSR is suitable for the environment where only a few sources communicate with infrequently accessed destinations, it may result in large delays and large communication overheads in highly dynamic environments. Therefore, DSR may have dynamic scalability problem. As the network becomes larger, control packets and message packets also become larger, since they need to carry the addresses of every node in the path. This may be a problem, since ad-hoc networks have limited available bandwidth. The protocol includes the entire route information in the data packet header which creates significant overhead as the route length increases. DSR also relies heavily on route caches to avoid repeated route discoveries. However, using stale route caches can adversely affect the performance of the protocol. If the routes are not updated a source node may use cached routes which are invalid due to mobility in the network. Intermediate nodes sending route replies using stale cached route could cause pollution of cached routes maintained at other nodes in the network.

5.2.B. TORA

TORA (Temporally-Ordered Routing Algorithm) is a highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. The actions taken by TORA like water flowing downhill toward a destination node through a network of tubes those models the routing state of the real network. Shortest path is considered of secondary importance, and longer routes are often used if discovery of newer routes could be avoided. TORA is also characterized by a multipath routing capability.

The protocol performs three basic functions:

1) Route creation where the nodes use the height metric to maintain a directed acyclic graph (DAG) based on the neighboring nodes;

2) Route maintenance where in case a DAG route is broken, it is necessary to re-establish a DAG rooted at the same destination;

3) Route erasure, where TORA floods a broadcast clear packet (CLR) throughout the network to erase invalid routes.

Though TORA has some efficient advantages but we didn't work with it because it didn't support in our system and create a lot of problems. TORA needs special support system that's why we work only with AODV and DSR for Reactive or on-demand routing protocols.

5.3. Hybrid (Combination of Reactive & Proactive Protocols)

It's a combination of both Proactive and Reactive protocols. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from Reactive protocol, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from Proactive protocol.

- AODV

5.3.A. AODV

Ad-hoc On-demand Distance Vector (AODV) is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It uses destination sequence numbers to ensure loop freedom at all times and by avoiding the Bellman-Ford "count-to-infinity" problem offers quick convergence when the ad hoc network topology changes

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies.
AODV uses a route discovery process to dynamically build new routes on an as need basis. AODV is a distributed algorithm using distance vector algorithms, such as the Bellman Ford algorithm. When a route to a destination is unknown, AODV creates a route request packet and broadcasts it to its neighbors. Route request messages contain the source ID, destination ID, source sequence numbers, destination sequence numbers, hop count and broadcast ID. The source sequence number and broadcast ID increment each time a new route request is generated. The destination sequence number is the source sequence number of the destination node as last recorded by the source node.

Each intermediate node receiving a route request caches the previous hop for the particular node originating the request; this helps to create a return path for the reply packets. AODV uses the destination sequence number to maintain freshness of routes. The destination node or any intermediate node can reply to a route request. If an intermediate node has previously learned the path to the destination node, it can reply with the next hop information only if it satisfies the following condition: the locally stored destination sequence number is higher or comparable to the destination sequence number in the route request packet. AODV relies heavily on the sequence numbers to avoid the count-to-infinity problem associated with distance vector protocols. The broadcast ID and source ID pair help in discarding any redundant requests that reach a node. The replying destination or intermediate node unicasts a route reply message to the specific source node that created the route request. Nodes receiving a route reply message store the source ID of the node forwarding the message as the next hop towards the destination in order to forward future traffic toward this destination. The hop count in each message is incremented by one at each forwarding node, which helps track the distance to the source or destination node

depending on the type of the message. A node generating a route request or route reply sets the hop count to zero, which is incremented at each intermediate forwarding node. This incrementing helps the intermediate node to determine the number of hops to reach the source or destination using the current path. The source node receiving a number of route replies from different paths uses the hop count in the route reply messages to choose the one with a lower hop count metric as the shortest route to the destination. Once a route is formed, AODV uses the current route until the route expires or any topology changes occur. Each node also maintains a *"precursor list"* [16] of nodes that help it identify the nodes it has to inform of a broken link. The "precursor list" is created from the route request packets and includes a list of nodes that are likely to use the current node as the next hop.

Each node monitors the status of each of its links, and when a link connectivity change occurs, the node creates a route error message and informs the members of the "precursor list" about the non-reachability of specific routes. AODV relies on medium access control (MAC) layer schemes or the use of beacon packets at periodic intervals to find the status of its directly connected neighbors. Topology changes or expiring timers associated with the route request, reply and beacon packets allow AODV to detect link failures.

AODV uses a progressive ring search technique to control the broadcast domain. Basically, it increases the time-to-live (TTL) value in each broadcast of the initial route request until it receives a route reply.

Example

Figure 5.3.A (i) depicts a network where in node 1 desires to communicate to node 8. The AODV modules running on node 1 flood the network with route request (RREQ) messages. Each node receiving a RREQ message stores the

previous hop and distance to source for the originating RREQ and forwards the RREQ to its neighbors.

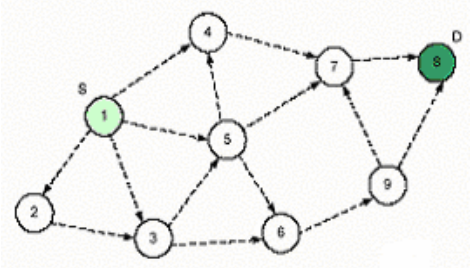


Figure 5.3.A (i): Route request (RREQ) flooding

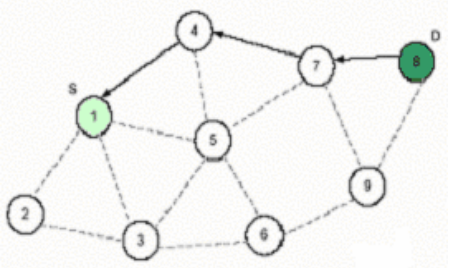


Figure 5.3.A (ii): Route reply propagation

When the RREQ message reaches the designation node 8, the destination sends a unicast route reply (RREP) message back to the source using the previous hop on which it received the RREQ. Each node receiving the RREP message in turn forwards it to the next hop with the smallest distance to the source as shown in Figure 5.3.A (ii). This process effectively builds the routing table at each node, and when any source destination pair establishes a route, the intermediate nodes learn the route as well.

Advantages and Disadvantages

The advantage of AODV is that it creates routes only on demand, which greatly reduces the periodic control message overhead associated with proactive routing protocols. The disadvantage is that there is route setup latency when a new route is needed, because ADOV queues data packets while discovering new routes and the queued packets are sent out only when new routes are found. This situation causes throughput loss in high mobility scenarios, because the packets get dropped quickly due to unstable route selection.

5.4. Other routing protocols

- Location based routing protocols

- Location aided routing protocols
- Expected zone and routing zone

6. Methodology

The simulations were performed using the latest release of Network Simulator2 (ns-2.3), particularly popular in the ad hoc networking community. NS-2 [19] is a discrete event simulator widely used in the networking research community. In general, the NS-2 installation will include all software extensions for simulating multi-hop wireless networks. It contains a detailed model of the physical and link layer behavior of a wireless network based on the 802.11 specifications and allows arbitrary movement of nodes within a network area. In NS-2 the user has to imagine of a scenario, the number of nodes to be placed in the scenario, and then write the TCL scripts (*.tcl* file) specifying the node configurations parameters and some other *ns* commands required to start and stop *ns*. The user has also to create the movement and connection files that together represent the scenario. The output of the simulation is a trace file (.tr), which is logged with each and every event that took place during the simulation. This file can than be used for obtaining measures such as mobility, throughput, end-to-end delay, and packet loss measurement. An optional output is the NAM [18] supported file (.nam) that logs the necessary events to help visualize the scenario using the NAM. The NAM is a post simulation process that shows how the nodes moved and how they were connected during the simulation. Another optional output is xgraph [18], which shows a graphical output for a specific measurement.

The AODV, DSR and DSDV protocols are also provided as part of the NS-2 installation.

7. SIMULATION Environment

The traffic sources are CBR (continuous bit –rate). The source-destination pairs are spread randomly over the network. The packet rate is 4 packets per

second for 3 and 9 sources, 3 packets per sec for 4 sources. The data packet size is 512 bytes. The mobility model uses *random waypoint model* in a rectangular filed of 500m x 400m with 9 nodes. In this mobility model, each node starts its journey from a fixed chosen location to a fixed chosen destination. Once the destination is reached it stop. From starting point to destination it chose its way randomly, after a pause time it go ahead to destination. The speed of nodes is varied between 5 to 10m/s and pause time was 1 seconds. But for the comparison on the basis of speed, node speed increases from 10 to 178m/s. Different network scenario for different numbers of node, pause time and speeds are generated. Simulations are run for 150 seconds. Transmission range was 250m and traffic type was TCP. Antenna was omni directional. The propagation model is the Two way ground model. Simulation parameters are listed in table 7.1.

Table: 7.1

Simulation Parameters

Parameter	**Value**
Simulator	ns-2
Studied protocols	DSDV, AODV, DSR
Antenna	Omni Directional
Simulation time	150 seconds
Simulation area	500 m x 400 m
Transmission range	250 m
Node movement model	Random waypoint
Speed	5 – 10 m/s
Traffic type	TCP
Data payload	200-2000 bytes/packet
Packet rate	100k-300k packets/sec
Node pause time	1 s

8. Performance Metrics

The following performance metrics are considered for evaluation:

8.1 Packet Delivery Fraction (PDF): The percentage ratio of the data packets delivered to the destinations to those generated by the sources [20]

8.2 Throughput: The ratio of the data packets delivered to the destinations to those generated by the sources [20].

8.3 Normalized routing load: The number of routing packets "transmitted" per data packet "delivered" at the destination [20].

9. SIMULATION METRICS

Simulation metrics are listed in Table 9.1.

Table: 9.1

ID	Metrics	Definition	Formula
PS	Packet sent	total number of packets sent by the source node	Computed from trace file
PR	Packet Received	Total number of packets Received by the Destination node	Computed from trace file
PDR	Packet delivery Ratio	Percentage of Throughput	PDR= (PR/PS)*100%
RF	Routing Packets	Number of routing packets sent or forwarded	Computed from trace file
NRL	Normalized Routing Load	Number of routing packets per data packets	NRL = RF/PR
TP	Throughput	Ratio of packets received to packets sent	TP= PR/PS

10. SIMULATION RESULTS

The simulation results are shown in the following section in the form of line graphs. Graphs show comparison between the three protocols by varying different numbers of sources on the basis of the above-mentioned metrics as a function of drop rate, received, send, time and speed.

10.1 A. Throughput:

Figure 10.1 shows a comparison between three routing protocols on the basis of throughput and packet size. Increasing the packet size 200 to 2000 for each protocol created 10 trace files, and from trace file calculated the out put for throughput. Receiving was much higher in AODV protocol than DSDV and DSR. Mean value for this case is AODV: 1.0355 DSDV: 1.0033 DSR: 1.0003. Performance of AODV is best here. DSDV performs better but another on demand protocol DSR performs worst.

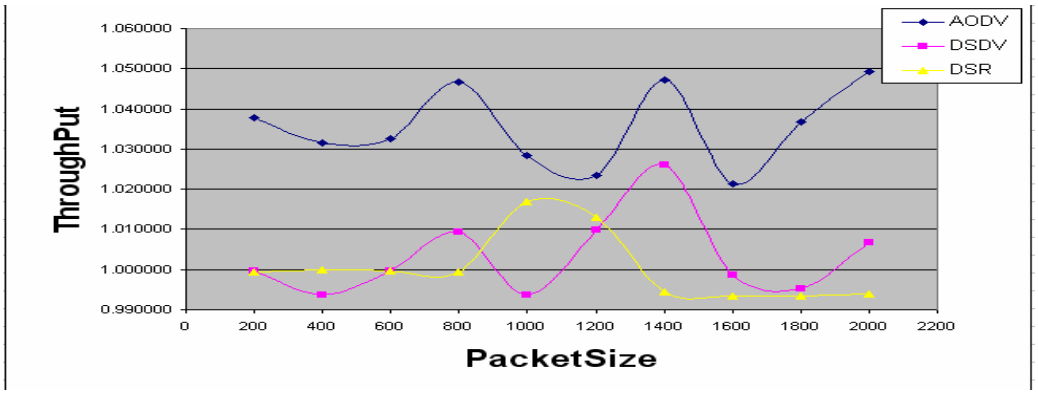


Figure: 10.1

Figure 10.2 shows a comparison between three routing protocols on the basis of throughput and time. Increasing the starting time 0.1 to 1.0 for each protocol created 10 trace files, and from trace file calculated the out put for throughput. Receiving was much higher in AODV protocol than DSDV and DSR. Mean value

for this case is AODV: 0.9923 DSDV: 0.9841 DSR: 0.9832. Performance of AODV is best here. DSR and DSDV performance was very close. But from the mean value, DSDV performs better but another on demand protocol DSR performs worst.

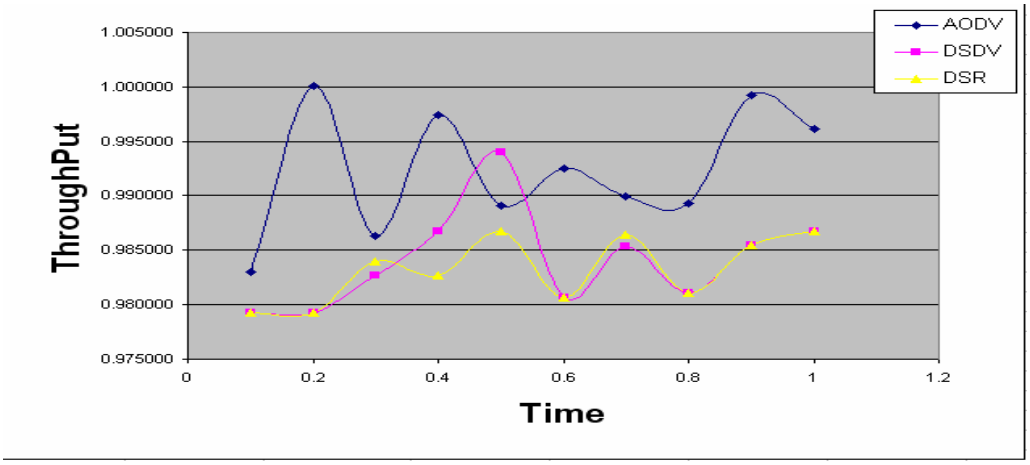


Figure: 10.2

Figure 10.3 shows a comparison between three routing protocols on the basis of throughput and speed. Increasing speed of the 9 nodes from 10 to 178 for each protocol, calculated the out put for throughput. The On-demand protocol, AODV performed particularly well, delivering almost 100% of the data packets regardless of the mobility rate. The packet delivery of AODV is almost independent of the number of sources that is varying number of sources does not effect AODV that much. DSR performance is worst when mobility is high. This poor performance is because of the reason that DSR can not work in high speed and high mobility, and it can not work with higher number of nodes. The packet delivery of DSDV protocol depends on the number of sources. Mean value for this case is AODV: 1.0099 DSDV: 1.0097 DSR: 0.8661. Performance of AODV and DSDV was very close. But DSR performs worst.

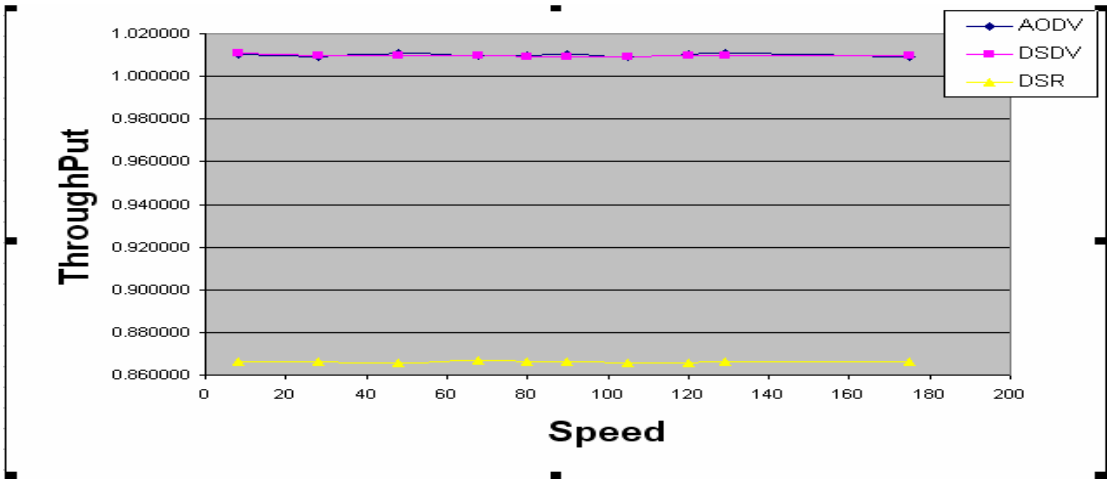


Figure: 10.3

Figure 10.4 and Figure: 10.5 shows a comparison between three routing protocols on the basis of Drop rate and speed, Drop rate and packet size. When increases the packet size drop rate for three protocols was almost same but from the mean value AODV: 1969.3 DSDV: 1920.1 DSR: 2086.9, it shows that DSR has the highest drop rate. Though DSR is an on demand protocol and it keeps multiple routes per destination, it has higher rate of packet drops. Mean value for Drop rate vs. Speed AODV: 376.9 DSDV: 405.7 DSR: 380.2. Here DSR drop rate is an average. As DSR can not work with high speed so it sending and receiving of packets is less than others here as a result drop rate is also less. It should not consider as a good performance.

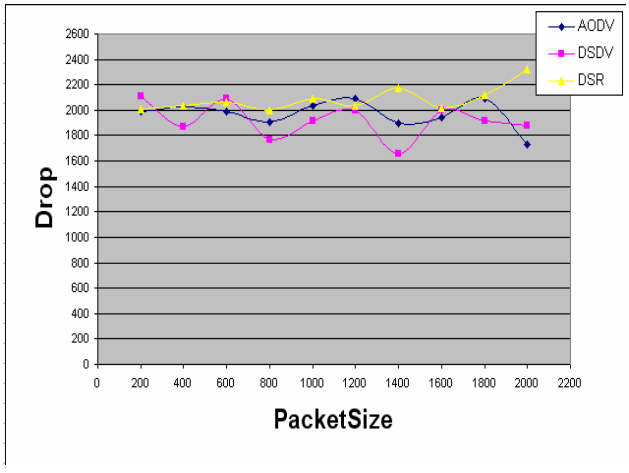


Figure: 10.4

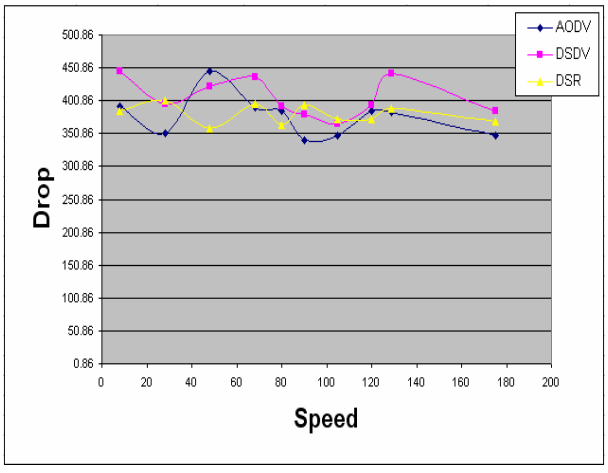


Figure: 10.5

10.2 B. Routing load:

Routing load measures the scalability of the protocols, how much overhead a protocol can take.

Figure 10.6 shows a comparison between both the routing protocols on the basis of normalized routing load as a function of time, using a different number of sources.

In case of AODV the normalized routing load drastically increases as the number of nodes increases. The routing load also increases as the node mobility increases. As the number of nodes increases, more nodes will be flooding the network with route request and consequently more nodes will be able to send route reply as well. As the node speed increases, a source node will have to generate more route requests to find a fresh enough route to destination node.

In case of DSDV the normalized routing load is almost the same with respect to node speed. The reason is that it is a table driven protocol, so a node does not need to find a route before transmitting packets. In case of DSR routing load was very low, it can not work with high speed so it can not take higher overhead.

Mean value for Routing load vs. Time AODV: 1.0148 DSDV: 1.0116 DSR: 0.8774.

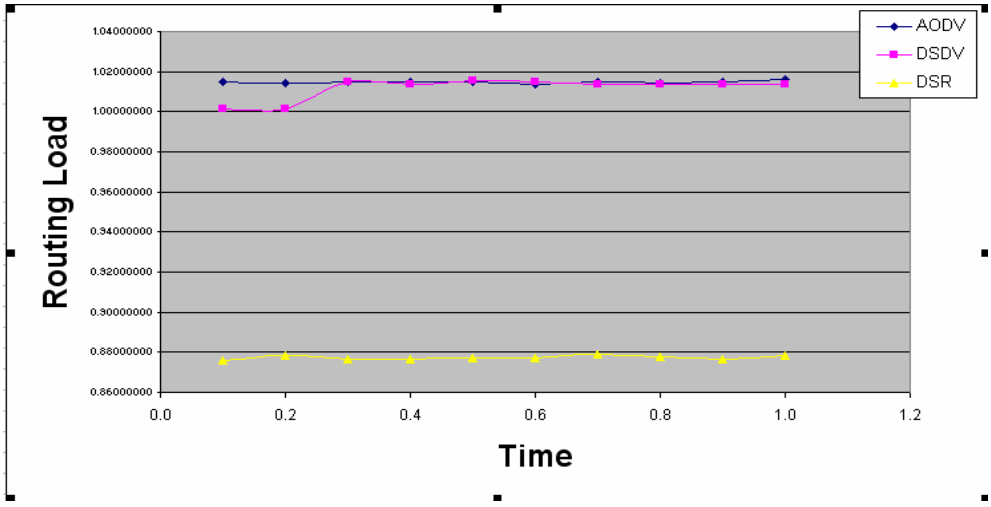


Figure: 10.6

10.3 C. Packet Delivery Ratio:

Packet delivery ratio is the percentage of throughput. For 9 nodes throughput is calculated in the basis of speed, time, and packet size. The On-demand protocol, AODV performed particularly well, delivering almost 95% of the data packets regardless of the mobility rate. The packet delivery of AODV is almost independent of the number of sources that is varying number of sources does not effect AODV that much. DSDV performed as well as AODV, delivering almost 90% of the data packets regardless of the mobility rate. DSR performs worst when mobility is high, and delivering almost 60% of the data packets.

Performance comparison based on the three parameters:

	Packet Delivery Ratio	Throughput	Routing Load
AODV	Best (95%)	Best	Best
DSDV	Better (90%)	Better	Better
DSR	Good (60%)	Better	Good

11. Congestion control in TCP

Congestion control in TCP [21] happens by three algorithms. They are Slow Start (Exponential Increase), Congestion Avoidance (Additive Increase), and Congestion Detection (Multiplicative Decrease). As we working with TCP New Reno, so after congestion detection it starts to follow a new algorithm which is first recovery. Each sender has a congestion window to control the flow of sending packets. In TCP congestion control starts with a Slow Start algorithm. In Slow Start the size of the window increase one maximum segment size (the

maximum segment size is determine during connection establishment) each time an acknowledgement is received. If the sender starts with cwnd=1, this means that the sender can send only one segment/byte. After receipt of the acknowledgement for segment 1, the size of the congestion window is increased by 1, which means cwnd=2 now the sender can send two more segment. By this way it increases but slow start can not continue indefinitely. So there is a threshold value called slow start threshold (ssthresh) to stop this phase. Initially the threshold value is equal to the maximum congestion window size. When the size of window reaches this threshold, slow start stop and now it decides whether it should go to congestion avoidance (additive increase) phase or congestion detection (multiplicative decrease) phase. Normally it starts with congestion avoidance phase. In this phase it try to avoid congestion so instead of increase window exponentially like slow start, it increase linearly. Like, after one segment is acknowledged it increase the window by two that means two more segments can send. After these two segments are acknowledged it increase the window by one. This time it can send only three more segments. If there is no acknowledgement comes, need to retransmit or duplicate acknowledgement comes the sender can assume that congestion happen. In this case, TCP NewReno starts a new phase called First Recovery. In First Recovery, at first it decreases the threshold value by half of the window size and start with the congestion avoidance phase. And try to find out which segment has not been acknowledged and need to retransmit. By this way it recovers and it remains in this phase until another time out or another duplicate acknowledgement comes.

11.1 Comparison based on congestion control:

Figure 11.1, 11.2 and shows congestion window vs. time for AODV DSR and DSDV protocols. When receiving and sending are smooth in the media congestion window is increasing and when media is busy and because of congestion dropping happen the congestion window is decreasing. In the figure

11.2 and 11.3 for DSR and DSDV the phase changing of increasing and decreasing is very frequent almost 4 or 5 times. In case of AODV congestion window increases and decrease after a long time and its changes phase only 3 times. So in this case AODV shows good performance in congestion control.

Figure: 11.1

Figure: 11.2

Figure: 11.3

12. NAM and XGRAPH

Figure 12.1, 12.2, and 12.3 shows the relationship between nam file and xgraph. These three figures are of same scenarios. In figure 12.2 it shows that at time 15.18029 sec packets are sending and receiving by the nodes and in the xgraph

which is figure 12.1 here at the same time congestion window is increasing. In figure: 12.3 for the same scenario at time 30.10036 because of congestion packets are dropping by the nodes and the xgraph, figure: 12.1 at the same time congestion window is decreasing.

Figure: 12.1

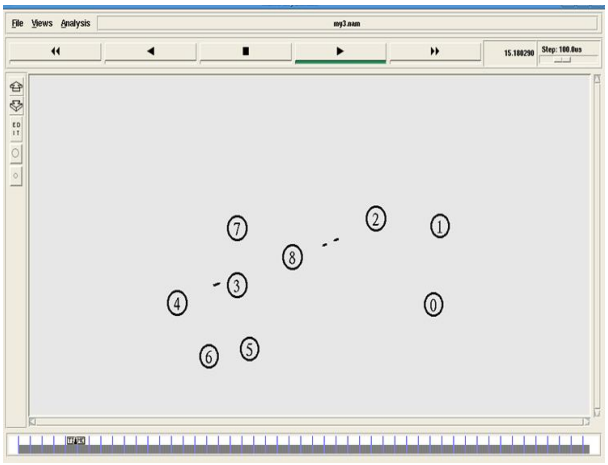


Figure: 12.2

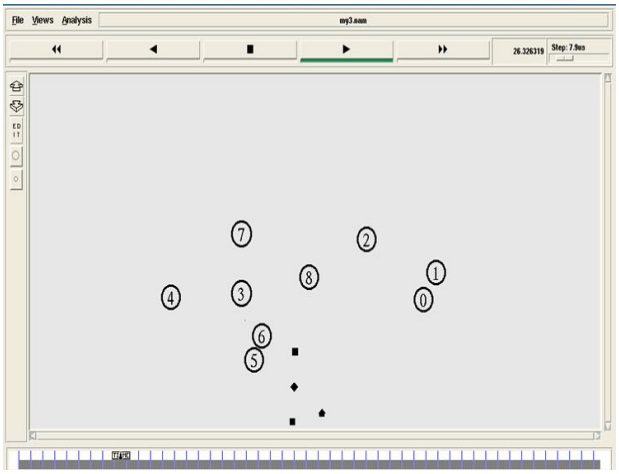


Figure: 12.3

13. Comparison based on Bandwidth

Bandwidth is the available capacity of the media for the nodes. Bandwidth was calculated for each protocol based on the channel capacity, how many bytes was

sending and receiving at a particular time and flow rate. Figure 13.1, 13.2, and 13.3 shows a comparison between three routing protocols on the basis of Bandwidth vs. Time. Total number of node was 9 but to make it easy to understand only three nodes bandwidth was shown in the figures. For node 3 which is blue color in the figure 13.1, 13.2 and 13.3, has highest bandwidth in all the three protocols. It shows a strong flow rate from starting to end in all the three protocols. In figure 13.1 which is DSDV, for node 2 (green color) in the starting its flow rate was very low but in the end it was good. In figure 13.2 which is DSR, for node 2 (green color) from the starting to end it was low but better than DSDV. In figure 13.3 which is AODV, for node 2 its performance is very low compare to other two protocols. Interesting thing happened for node 1 which is red color in the figure 13.1, 13.2 and 13.3. In figure 13.1 DSDV, its performance is good, same for AODV (figure 13.3). But figure 13.2 which is for DSR, it starts late but in the beginning its performance was very high compare to other protocols. But after a certain point its performance was almost zero till end. Its flow rate was very low and after a long time it sends small amount of packets. So for DSR bandwidth is poor than the other protocols.

Figure: 13.1

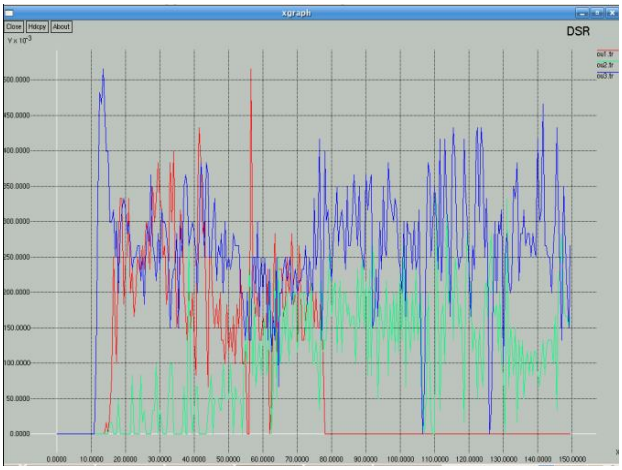
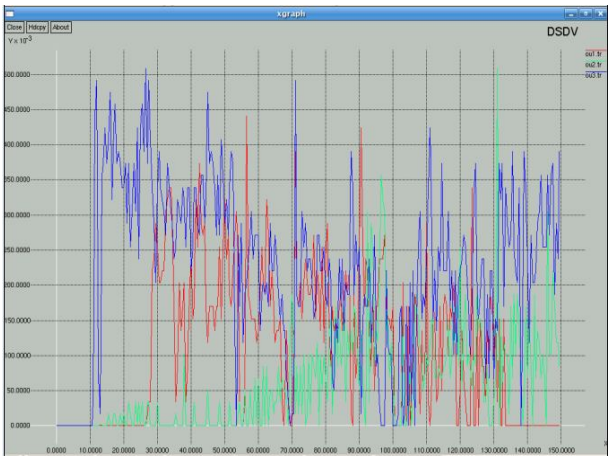


Figure: 13.2



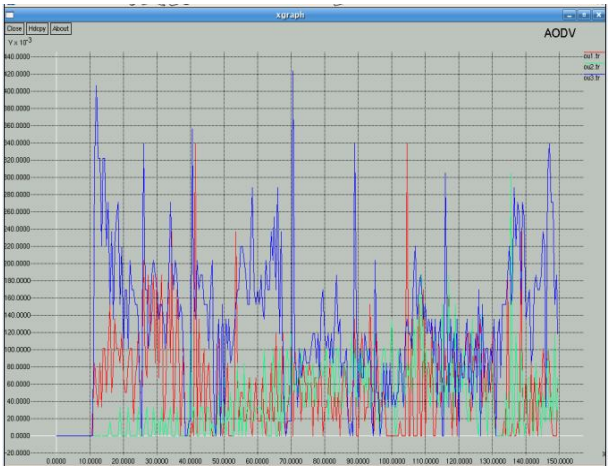


Figure: 13.3

14. Overall Performance Comparison

Performance comparison based on packet delivery ratio, throughput, bandwidth, congestion control, drop rate, normalized routing overload, in almost every case AODV performs best in all mobility. DSDV performs well but as it is not an on demand protocol, so it always has to be updated. DSR was better but it can not work more than 200 nodes, it needs all the nodes very close to each other.

AODV	Best
DSDV	Better
DSR	Better (Not more than 200 nodes)

15. Conclusion

Using ns2, results were presented of a detailed packet-level simulation of three protocols.

This paper compared the three ad hoc routing protocols. AODV and DSR, are On – Demand routing protocols, and DSDV a table driven protocol.

Simulation results show that all of the protocols deliver a greater percentage of the originated data packets when there is little node mobility, converging to 100% delivery ration when there is no node motion. The packet delivery of AODV is almost independent of the number of sources. DSDV generates less routing load then AODV. DSR packet delivery ratio is very low for high mobility scenarios. Packet delivery ratio of all the protocols decreases as speed increases, but DSR's packet delivery ratio decreases in a steeper and more rapid fashion. AODV has less average end-to-end delay when compared to DSDV. The normalized routing load for AODV increases drastically as the number of nodes increases. The routing load also increases as the node speed increases. But for DSDV the normalized routing load is almost the same with respect to node speed. The routing load was very low for DSR. Its performance was very poor as node speed increases.

So in conclusion, AODV was very good at all mobility rates and movement speeds. DSDV performs almost as well as AODV. And DSDV delivered virtually all packets at good node mobility. DSR performs predictably, but still requires the transmission of many routing overhead packets and it failing to converge as node mobility increases.

16. Future Work

The congestion control algorithm in TCP NewReno, every sender waits for acknowledgement for each segment or bytes. It is one of the reasons for making network slower. Because the segment could be loss or the acknowledgement

could be loss. And retransmission is one of the reasons of congestion. So our focus will be, try to improve network capacity by sending acknowledgement for group of segments instead of one acknowledgement for one segment.
Another thing we find out while doing this thesis, in the back-off algorithm each sender has to wait for exponential time to send one segment though the channel is idle. This time can not keep fixed because of hidden node problem. So, our future work will focus to change this exponential time to polynomial time without allowing any hidden node problem or exposed node problem.

REFERENCES

[1] W. F. Lo and H.T. Mouftah. Carrier Sense Multiple Access with Collision Detection for Radio Channels. IEEE 13th Intl. Commun. and Energy Conf., 1984.

[2] R. Rom. Collision Detection in Radio Channels. Local Area and Multiple Access Networks. Computer science Press, 1986.

[3] F.A. Tobagi and L. Kleinrock. Packet Switching in Radio Channels: Part II - The Hidden Terminal Problem in Carrier Sense Multiple Access Modes and The Busy-Tone Solution. IEEE Transactions on Communications, COM-23(12), 1975.

[4] F. Talucci, M. Gerla, and L. Fratta. MACA-BI (MACA by Invitation)-A Receiver Oriented Access Protocol for Wireless Multihop Networks. In Proc. of IEEE PIMRC '97 [Compressed Postscript]

[5] H. Chhaya and S. Gupta. Throughput and Fairness Properties of Asynchronous Data Transfer Methods in the IEEE 802.11 MAC Protocol. In proc. Sixth International Conference on Personal, Indoor and Mobile Radio Communications, 1996.

[6] ETSI Web Page. http://www.etsi.org/technicalactiv/h1tech.htm.

[7] V. Bhargavan, A. Demers, S. Shenker, and L Zhang. MACAW: A Media Access Protocol for Wireless LAN's. In Proc., ACM SIGCOMM' 94.

[8] Tanenbaum, A.S., "*Computer Networks*", 3rd Edition, Prentice Hall (1996)

[9] Schiller, J., "*Mobile Communication*", 2nd Edition, Addison Wesley (2003)

[10] Rappaport, T.S., "*Wireless Communication principle and practice*", 2nd Edition, Prentice Hall (1996)

[11] Kurose, J.F., Ross, K.W., "*Computer Networking - A Top Down Approach*", 3rd Edition,Addison Wesley (2004)

[12] V. Bhargavan, A. Demers, S. Shenker, and L Zhang. MACAW: A Media Access Protocol for Wireless LAN's. In Proc., ACM SIGCOMM' 94.

[13] Chane L. Fullmer, and J. J. Garcia-Luna-Aceves. Floor acquisition multiple access (FAMA) for Packet-Radio networks. In Proc. SIGCOMM' 95.

[14] Chane L. Fullmer, and J. J. Garcia-Luna-Aceves. Solutions to Hidden Terminal Problems in Wireless Networks. In Proc. SIGCOMM' 97.

[15] Zygmunt J. Haas, Jing Deng, "*Dual busy tone multiple access (DBTMA) - a multiple access control scheme for ad hoc networks"*, IEEE Transactions on Communications, Vol. 50, Pages: 975 – 985, June 2002

[16] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network," *Ericsson Review*, No.4, 2000, pp. 248-263.

[17] IETF Working Group: Mobile Adhoc Networks (manet). http://www.ietf.org/html.charters/manet-charter.html.

[18] http://www.isi.edu/nsnam/

[19] http://evanjones.ca/ns2.html

[20] http://www.cs.umu.se/education/examina/Rapporter/

[21] Behrouz A Frouzan, Data Communication and Networking